United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. EDT
Wednesday, May 21, 2008

INFORMATION SECURITY

TVA Needs to Enhance Security of Critical Infrastructure Control Systems and Networks

Statement of Gregory C. Wilshusen
Director, Information Security Issues

Nabajyoti Barkakati
Acting Chief Technologist

May 21, 2008

INFORMATION SECURITY

TVA Needs to Enhance Security of Critical Infrastructure Control Systems and Networks

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-775T, a testimony before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

The control systems that regulate the nation's critical infrastructures face risks of cyber threats, system vulnerabilities, and potential attacks. Securing these systems is therefore vital to ensuring national security, economic well-being, and public health and safety. While most critical infrastructures are privately owned, the Tennessee Valley Authority (TVA), a federal corporation and the nation's largest public power company, provides power and other services to a large swath of the American Southeast.

GAO was asked to testify on its public report being released today on the security controls in place over TVA's critical infrastructure control systems. In doing this work, GAO examined the security practices in place at TVA facilities; analyzed the agency's information security policies, plans, and procedures in light of federal law and guidance; and interviewed agency officials responsible for overseeing TVA's control systems and their security.

What GAO Recommends

In public and limited distribution reports being issued today, GAO is recommending that TVA take steps to improve implementation of the agency's information security program and to correct specific security weaknesses identified at TVA facilities.

In comments on drafts of GAO's reports, TVA provided information on steps it is taking to implement these recommendations.

To view the full product, including the scope and methodology, click on GAO-08-775T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

TVA had not fully implemented appropriate security practices to secure the control systems used to operate its critical infrastructures at facilities GAO reviewed. Multiple weaknesses within the TVA corporate network left it vulnerable to potential compromise of the confidentiality, integrity, and availability of network devices and the information transmitted by the network. For example, almost all of the workstations and servers that GAO examined on the corporate network lacked key security patches or had inadequate security settings. Furthermore, TVA did not adequately secure its control system networks and devices on these networks, leaving the control systems vulnerable to disruption by unauthorized individuals. Network interconnections provided opportunities for weaknesses on one network to potentially affect systems on other networks. For example, weaknesses in the separation of network segments could allow an individual who gained access to a computing device connected to a less secure portion of the network to compromise systems in a more secure portion of the network, such as the control systems. In addition, physical security at multiple locations that GAO reviewed did not sufficiently protect the control systems. For example, live network jacks connected to TVA's internal network at certain facilities GAO reviewed had not been adequately secured from unauthorized access. As a result, TVA's control systems were at increased risk of unauthorized modification or disruption by both internal and external threats.

An underlying reason for these weaknesses was that TVA had not consistently implemented significant elements of its information security program. For example, the agency lacked a complete and accurate inventory of its control systems and had not categorized all of its control systems according to risk, limiting assurance that these systems are adequately protected. In addition, TVA's patch management process lacked a mechanism to effectively prioritize vulnerabilities. As a result, patches that were identified as critical, meaning they should be applied immediately to vulnerable systems, were not applied in a timely manner.

Numerous opportunities exist for TVA to improve the security of its control systems. For example, TVA can strengthen logical access controls, improve physical security, and fully implement its information security program. If TVA does not take sufficient steps to secure its control systems and fully implement an information security program, it risks not being able to respond properly to a major disruption that is the result of an intended or unintended cyber incident.

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to participate in today's hearing to discuss control systems security. We have previously reported and testified before this subcommittee that critical infrastructure control systems face increasing risks due to cyber threats, system vulnerabilities, and the serious potential impact of attacks as demonstrated by reported incidents.[1] If control systems are not adequately secured, their vulnerabilities could be exploited, and our critical infrastructures could be disrupted or disabled, possibly resulting in loss of life, physical damage, or economic losses.

The majority of our nation's critical infrastructures are owned by the private sector; however, the federal government owns and operates critical infrastructure facilities including ones used for energy, water treatment and distribution, and transportation. One such entity, the Tennessee Valley Authority (TVA)—a federal corporation and the nation's largest public power company—generates electricity using its 52 fossil, hydro, and nuclear facilities, all of which use control systems. As a wholly-owned government corporation, TVA is to comply with the Federal Information Security Management Act of 2002[2] (FISMA) by developing a risk-based information security program and implementing appropriate information security controls for its computer systems.

In our testimony today, we will summarize the results of our review of the security controls over TVA's critical infrastructure control systems. We are issuing two reports today, one publicly available and one with limited distribution, which provide additional details on the results of our review.[3] Our objective was to determine

[1]GAO, *Critical Infrastructure Protection: Federal Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, GAO-07-1036 (Washington, D.C.: September 2007) and GAO, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*. GAO-08-119T (Washington, D.C.: October 2007).

[2]FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347 (Dec.17, 2002).

[3]GAO, *Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks*, GAO-08-459SU and GAO-08-526 (Washington, D.C.: May 2008).

whether TVA has effectively implemented appropriate information security practices for its control systems. In preparing for this testimony, we relied on our work supporting these reports, which discuss the details of our scope and methodology. The information in this testimony is specifically based on our public report, which has been reviewed for sensitivity by TVA.

Our testimony is based on the work done for our reports from March 2007 to May 2008. The work on which this testimony is based was conducted in accordance with generally accepted government auditing standards, which require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Results in Brief

TVA had not fully implemented appropriate security practices to secure the control systems used to operate its critical infrastructures at facilities we reviewed. Specifically, network interconnections provided opportunities for weaknesses on one network to potentially affect systems on other networks. For example, weaknesses in the separation of network segments could allow an individual who gained access to a computing device connected to a less secure portion of the network to compromise systems in a more secure portion of the network, such as the control systems. In addition, physical security at multiple locations that we reviewed did not sufficiently protect the control systems. As a result, TVA's control systems were at increased risk of unauthorized modification or disruption by both internal and external threats.

An underlying reason for these weaknesses was that TVA had not consistently implemented significant elements of its information security program. For example, the agency lacked a complete and accurate inventory of its control systems and it had not categorized all of its control systems according to risk, limiting assurance that these systems were adequately protected. In addition, TVA's patch

management process lacked a mechanism to effectively prioritize vulnerabilities. Until TVA fully and consistently implements its information security program, it risks a disruption of its operations, which could impact both TVA and its customers.

In the reports being issued today,[4] we are making 19 recommendations to the Chief Executive Officer of TVA to improve the implementation of its agencywide information security program and 73 recommendations to correct specific information security weaknesses.

In its comments on our reports, TVA concurred with all of our recommendations regarding its information security program and the majority of our recommendations regarding specific information security weaknesses and provided information on steps the agency was taking to implement our GAO recommendations.

Background

Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. Of particular importance is the security of information and systems supporting critical infrastructures--physical or virtual systems and assets so vital to the nation that their incapacitation or destruction would have a debilitating impact on national and economic security and on public health and safety. Although the majority of our nation's critical infrastructures are owned by the private sector, the federal government owns and operates key facilities that use control systems, including oil, gas, water, electricity, and nuclear facilities. In the electric power industry, control systems can be used to manage and control the generation, transmission, and distribution of electric power. For example, control systems can open and close circuit breakers and set thresholds for preventive shutdowns.

[4]GAO-08-526 and GAO-08-459SU.

Critical infrastructure control systems face increasing risks due to cyber threats, system vulnerabilities, and the potential impact of attacks as demonstrated by reported incidents.[5] Control systems are more vulnerable to cyber threats and unintended incidents now than in the past for several reasons, including their increasing standardization and connectivity to other systems and the Internet. For example, in August 2006, two circulation pumps at Unit 3 of the Browns Ferry, Alabama, nuclear power plant operated by TVA failed, forcing the unit to be shut down manually. The failure of the pumps was traced to an unintended incident involving excessive traffic on the control system's network.

To address this increasing threat to control systems governing critical infrastructures, both federal and private organizations have begun efforts to develop requirements, guidance, and best practices for securing those systems. For example, FISMA outlines a comprehensive risk-based approach to securing federal information systems, which include control systems. Federal organizations, including the National Institute of Standards and Technology (NIST), the Federal Energy Regulatory Commission (FERC), and the Nuclear Regulatory Commission (NRC), have used a risk-based approach to develop guidance and standards to secure control systems. NIST guidance has been developed that currently applies to federal agencies; however, much of the guidance and standards developed by FERC and NRC has not yet been finalized. Once implemented, FERC and NRC standards will apply to both public and private organizations that operate covered critical infrastructures.

TVA Provides Power to the Southeastern United States

The TVA is a federal corporation and the nation's largest public power company. TVA's power service area includes almost all of Tennessee and parts of Mississippi, Kentucky, Alabama, Georgia, North Carolina, and Virginia. It operates 11 coal-fired fossil plants, 8 combustion turbine plants, 3 nuclear plants, and a hydroelectric

[5]See GAO, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, GAO-07-1036 (Washington, D.C.: Sept. 10, 2007).

system that includes 29 hydroelectric dams and one pumped storage facility.[6] TVA also owns and operates one of the largest transmission systems in North America.

Control systems are essential to TVA's operation because it uses them to both generate and deliver power. To generate power, control systems are used within power plants to open and close valves, control equipment, monitor sensors, and ensure the safe and efficient operation of a generating unit. Many control systems networks connect with other agency networks to transmit system status information. To deliver power, TVA monitors the status of its own and surrounding transmission facilities from two operations centers.

TVA Had Not Fully Implemented Appropriate Controls to Protect Control Systems from Unauthorized Access

TVA had not fully implemented appropriate security practices to secure the networks on which its control systems rely. Specifically, the interconnected corporate and control systems networks at certain facilities that we reviewed did not have sufficient information security safeguards in place to adequately protect control systems. In addition, TVA did not always implement controls adequate to restrict physical access to control system areas and to protect these systems—and their operators—from fire damage or other hazards. As a result TVA, control systems were at increased risk of unauthorized modification or disruption by both internal and external threats.

Weaknesses in TVA's Corporate Network Controls Placed Network Devices at Risk

Multiple weaknesses within the TVA corporate network left it vulnerable to potential compromise of the confidentiality, integrity,

[6]A pumped-storage plant uses two reservoirs, with one located at a much higher elevation than the other. During periods of low demand for electricity, such as nights and weekends, energy is stored by reversing the turbines and pumping water from the lower to the upper reservoir. The stored water can later be released to turn the turbines and generate electricity as it flows back into the lower reservoir.

and availability of network devices and the information transmitted by the network. For example:

- Almost all of the workstations and servers that we examined on the corporate network lacked key security patches or had inadequate security settings.
- TVA hd not effectively configured host firewall controls on laptop computers we reviewed, and one remote access system that we reviewed had not been securely configured.
- Network services had been configured across lower and higher-security network segments, which could allow a malicious user to gain access to sensitive systems or modify or disrupt network traffic.
- TVA's ability to use its intrusion detection system[7] to effectively monitor its network was limited.

Weaknesses in TVA Control Systems Networks Jeopardized the Security of its Control Systems

The access controls implemented by TVA did not adequately secure its control systems networks and devices, leaving the control systems vulnerable to disruption by unauthorized individuals. For example:

- TVA had implemented firewalls to segment control systems networks from the corporate network. However, the configuration of certain firewalls limited their effectiveness.
- The agency did not have effective passwords or other equivalent documented controls to restrict access to the control systems we reviewed. According to agency officials, passwords were not always technologically possible to implement, but in the cases we reviewed there were no documented compensating controls.

[7]An intrusion detection system detects inappropriate, incorrect, or anomalous activity that is aimed at disrupting the confidentiality, availability, or integrity of a protected network and its computer systems.

- TVA had not installed current versions of patches for key applications on computers on control systems networks. In addition, the agencywide policy for patch management did not apply to individual plant-level control systems.

- Although TVA had implemented antivirus software on its transmission control systems network, it had not consistently implemented antivirus software on other control systems we reviewed.

Physical Security Did Not Sufficiently Protect Sensitive Control Systems

TVA had not consistently implemented physical security controls at several facilities that we reviewed. For example:

- Live network jacks connected to TVA's internal network at certain facilities we reviewed had not been adequately secured from unauthorized access.

- At one facility, sufficient emergency lighting was not available, a server room had no smoke detectors, and a control room contained a kitchen (a potential fire and water hazard).

- The agency had not always ensured that access to sensitive computing and industrial control systems resources had been granted to only those who needed it to perform their jobs. At one facility, about 75 percent of facility badgeholders had access to a plant computer room, although the vast majority of these individuals did not need access. Officials stated that all of those with access had been through the required background investigation and training process. Nevertheless, an underlying principle for secure computer systems and data is that users should be granted only those access rights and permissions needed to perform their official duties.

Information Security Management Program Was Not Consistently Implemented Across TVA's Critical Infrastructure

An underlying reason for TVA's information security control weaknesses was that it had not consistently implemented significant elements of its information security program, such as: documenting

a complete inventory of systems; assessing risk of all systems identified; developing, documenting, and implementing information security policies and procedures; and documenting plans for security of control systems as well as for remedial actions to mitigate known vulnerabilities. As a result of not fully developing and implementing these elements of its information security program, TVA had limited assurance that its control systems were adequately protected from disruption or compromise from intentional attack or unintentional incident.

TVA's Inventory of Systems Did Not Include Many Control Systems

TVA's inventory of systems did not include all of its control systems as required by agency policy. In its fiscal year 2007 FISMA submission, TVA included the transmission and the hydro automation control systems in its inventory. However, the plant control systems at its nuclear and fossil facilities had not been included in the inventory. At the conclusion of our review, agency officials stated they planned to develop a more complete and accurate system inventory by September 2008.

TVA Had Not Assessed Risks to Its Control Systems

TVA had not completed categorizing risk levels or assessing the risks to its control systems. FISMA mandates that agencies assess the risk and magnitude of harm that could result from the unauthorized access, use, disclosure disruption, modification, or destruction of their information and information systems. However, while the agency had categorized the transmission and hydro automation control systems as high-impact systems,[8] its nuclear division and fossil business unit, which includes its coal and combustion turbine facilities, had not assigned risk levels to its control systems. TVA had also not completed risk assessments for the control systems at its hydroelectric, nuclear, coal, and combustion turbine facilities. According to TVA officials, the agency plans to complete the hydroelectric and nuclear control systems risk assessments by June 2008 and they plan to complete the security

[8]Federal Information Processing Standard 199 provides criteria for categorizing risk to systems as high, moderate, or low.

categorization of remaining control systems throughout TVA by September 2008, except for fossil systems, for which no date has been set.

Inconsistent Application of TVA's Policies and Procedures Contributed to Program Weaknesses

Several shortfalls in the development, documentation, and implementation of TVA's information security policies contributed to many of the inadequacies in TVA's security practices. For example:

- TVA had not consistently applied agencywide information security policies to its control systems, and TVA business unit security policies were not always consistent with agencywide information security policies.
- Cyber security responsibilities for interfaces between TVA's transmission control system and its hydroelectric and fossil generation units had not been documented.
- Physical security standards for control system sites had not been finalized or were in draft form.

Patch Management Weaknesses Left TVA's Control Systems Vulnerable

Weaknesses in TVA's patch management process hampered the efforts of TVA personnel to identify, prioritize, and install critical software security patches to TVA systems in a timely manner. For a 15-month period, TVA documented its analysis of 351 reported vulnerabilities, while NIST's National Vulnerability Database[9] reported about 2,000 vulnerabilities rated as high or medium risk for the types of systems in operation at TVA for the same time period. In addition, upon release of a patch by the software vendor, the agency had difficulty in determining the patch's applicability to the software applications in use at the agency because it did not have a mechanism in place to provide timely access to software version and configuration information for the applications. Furthermore,

[9]The National Vulnerability Database is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance.

TVA's written guidance on patch management provided only limited guidance on how to prioritize vulnerabilities. The guidance did not refer to the criticality of IT resources or specify situations in which it was acceptable to upgrade or downgrade a vulnerability's priority from that given by its vendors or third-party patch tracking services. For example, agency staff had reduced the priority of three vulnerabilities identified as critical or important by the vendor or a patch tracking service and did not provide sufficient documentation of the basis for this decision. As a result, patches that were identified as critical were not applied in a timely manner; in some cases, a patch was applied more than 6 months past TVA deadlines for installation.

TVA Had Not Developed System Security and Remedial Action Plans for All Control Systems

TVA had not developed system security or remedial action plans for all control systems as required under federal law and guidance. Security plans document the system environment and the security controls selected by the agency to adequately protect the system. Remedial action plans document and track activities to implement missing controls such as missing system security plans and other corrective actions necessary to mitigate vulnerabilities in the system. Although TVA had developed system security and remedial action plans for its transmission control system, it had not done so for control systems at the hydroelectric, nuclear, or fossil facilities. According to agency officials, TVA plans to develop a system security plan for its hydroelectric automation and nuclear control systems by June 2008, but no time frame has been set to complete development of a security plan for control systems at fossil facilities. Until the agency documents security plans and implements a remediation process for all control systems, it will not have assurance that the proper controls will be applied to secure control systems or that known vulnerabilities will be properly mitigated.

Opportunities Exist to Improve Security of TVA's Control Systems

Numerous opportunities exist for TVA to improve the security of its control systems. Specifically, strengthening logical access controls over agency networks can better protect the confidentiality, integrity, and availability of control systems from compromise by

unauthorized individuals. In addition, fortifying physical access controls at its facilities can limit entry to TVA restricted areas to only authorized personnel, and enhancing environmental safeguards can mitigate losses due to fire or other hazards. Further, establishing an effective information security program can provide TVA with a solid foundation for ensuring the adequate protection of its control systems.

Because of the interconnectivity between TVA's corporate network and certain control systems networks, we recommend that TVA implement effective patch management practices, securely configure its remote access system, and appropriately segregate specific network services. We also recommend that the agency take steps to improve the security of its control systems networks, such as implementing strong passwords or equivalent authentication mechanisms, implementing antivirus software, restricting firewall configuration settings, and implementing equivalent compensating controls when such steps cannot be taken.

To prevent unauthorized physical access to restricted areas surrounding TVA's control systems, we recommend that the agency take steps to toughen barriers at points of entry to these facilities. In addition, to protect TVA's control systems operators and equipment from fire damage or other hazards, we also recommend that the agency improve environmental controls by enhancing fire suppression capabilities and physically separating cooking areas from system equipment areas.

Finally, to improve the ability of TVA's information security program to effectively secure its control systems, we are recommending that the agency improve its configuration management process and enhance its patch management policy. We also recommend that TVA complete a comprehensive system inventory that identifies all control systems, perform risk assessments and security risk categorization of these systems, and document system security and remedial action plans for these systems. Further, we recommend improvements to agency information security policies.

In commenting on drafts of our reports, TVA concurred with all of our recommendations regarding its information security program

and the majority of our recommendations regarding specific information security weaknesses. The agency agreed on the importance of protecting critical infrastructures and stated that it has taken several actions to strengthen information security for control systems, such as centralizing responsibility for cyber security within the agency. It also provided information on steps the agency was taking to implement certain GAO recommendations.

In summary, TVA's power generation and transmission critical infrastructures are important to the economy of the southeastern United States and the safety, security, and welfare of millions of people. Control systems are essential to the operation of these infrastructures; however, multiple information security weaknesses exist in both the agency's corporate network and individual control systems networks and devices. An underlying cause for these weaknesses is that the agency had not consistently implemented its information security program throughout the agency. If TVA does not take sufficient steps to secure its control systems and implement an information security program, it risks not being able to respond properly to a major disruption that is the result of an intended or unintended cyber incident.

Mr. Chairman, this concludes our statement. We would be happy to answer questions at this time.

Contact and Staff Acknowledgments

If you have any questions regarding this testimony, please contact Gregory C. Wilshusen, Director, Information Security Issues, at (202) 512-6244 or wilshuseng@gao.gov, or Nabajyoti Barkakati, Acting Chief Technologist, at (202) 512-4499 or barkakatin@gao.gov.

Other key contributors to this testimony include Nancy DeFrancesco and Lon Chin (Assistant Directors); Angela Bell; Bruce Cain; Mark Canter; Heather Collins; West Coile; Kirk Daubenspeck; Neil Doherty; Vijay D'Souza; Nancy Glover; Sairah Ijaz; Myong Kim;

Stephanie Lee; Lee McCracken; Duc Ngo; Sylvia Shanks; John Spence; and Chris Warweg.